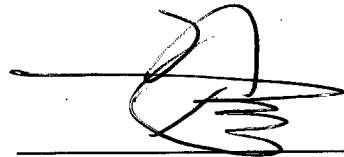


VERIFICATION OF TRANSLATION

I, KIM Yoo, a Patent Attorney, of Suite 202 Taewon Building, 746-15
Yoksam-dong, Kangnam-gu, Seoul, 135-080, Korea, hereby declare as
follows:

1. I am a translator and am familiar with English language.
2. I am the translator of the documents attached hereto, English
translations of the Korean Patent Publication Number. 2003-0083102, and
certify that the following is a true translation to the best of my knowledge
and belief.

Dated this 24th day of August 2006



Signature of Translator

(19) Korean Industrial Property Office (KR)

(12) Published patent Gazette (A)

(51) . Int. Cl. ⁷

(11) Publication No.: Pat. 2003-0083102

5 H04K 1/04

(43) Publication Date: Oct. 30, 2003

(21) Application No.: 10-2002-0021506

(22) Filing Date: Apr. 19, 2002

10

(71) Applicant: Electronics and Telecommunications Research Institute
161 Gajeong-dong, Yuseong-gu, Daejeon

(72) Inventor SON, Young-Ho
203-205 Songgang Maeul Apartment, Songgang-dong
Yuseong-gu Daejeon

15

(74) Agent Patent Attorney SHIN, Young-Moo

Request for Examination: Yes

20 (54) METHOD OF SCRAMBLING AND DESCRAMBLING USING FAST FOURIER
TRANSFORM

ABSTRACT

25 Disclosed relates to a method of fast Fourier transform scrambling and
descrambling that scales the amplitude of signal in the fast Fourier transform pursuant to a
substitution table produced in a transmission part in real time and, then, scrambles the
location of frequency component to modulate the location of frequency component as well
as the amplitude of frequency component, differently from the conventional fast Fourier
30 transform method that scrambles only the location of frequency component pursuant to a
substitution table generated, thus reducing much more the residual intelligibility of the
original signal and improving the safety of analog scrambler.

REPRESENTATIVE DRAWING

35 Fig. 2

KEY WORDS

Fast Fourier Transform, Amplitude Scaling, Residual Intelligibility, Substitution Table, Scaling

5

SPECIFICATION

Brief Description of the Drawings

Fig. 1 is a conceptual diagram depicted for illustrating a conventional method of fast Fourier transform scrambling and descrambling;

10

Fig. 2 is a conceptual diagram depicted for illustrating a method of fast Fourier transform scrambling and descrambling in accordance with the present invention;

Fig. 3 is a conceptual diagram depicted for illustrating an amplitude scaling operation of a transmission part in detail; and

Fig. 4 is a conceptual diagram depicted for illustrating an amplitude restoring operation of a reception part in detail.

15

<Description of Major Elements in the above Figures>

10 & 20: Scrambling process

11 & 20: Descrambling process

20 Detailed Description of the Invention

Object of the Invention

Description of the Related Art

The present invention relates to a method of fast Fourier transform scrambling and descrambling and, more particularly, to a method of fast Fourier transform scrambling and descrambling that reduces the residual intelligibility of an original signal existing scrambled analog signals.

25

A fast Fourier transform (hereinafter, referred to as FFT) scrambling is to conceal information implied in a random real signal when the signal is transmitted.

The FFT scrambling method is one of the generally used analog scrambling methods. Such FFT scrambling method is applicable to an analog scrambler, which directly permutes an analog voice, for protecting an end-to-end voice communication in a public switched telephone network (PSTN) and the like. The FFT scrambling method can reduce the residual intelligibility much more than existing analog scrambling methods

30

when tapping the scrambled voice in a transmission channel.

The method of scrambling a voice in the FFT scrambler executes a fast Fourier transform for an input voice signal, substitutes the locations of frequency components pursuant to a substitution table generated by a specific code algorithm in real time, then,
 5 carries out an inverse FFT (IFFT) to transmit the voice signal to a channel in the form of an analog signal.

Hereinafter, the method of fast Fourier transform scrambling and descrambling in accordance with the conventional art will now be described with reference to the attached drawings.

10 Fig. 1 is a conceptual diagram depicted for illustrating a conventional method of fast Fourier transform scrambling and descrambling.

Referring to the figure, in a scrambling process 10 of a transmission part, a real signal (101), an analog signal, of time domain input to a transmission end is sampled by an appropriate sampling frequency based on the sampling theorem, thus being converted
 15 into a digital signal (102).

Data generated as a result of an analog to digital (A/D) conversion is a discrete signal expressed in the unit of bit quantized when sampling. Such signal will be a sample data, i.e., a data unit to be processed digitally. The digital-converted data is converted into a frequency domain signal by executing an N-point FFT (103). The signal coefficient
 20 of frequency domain expressed by a complex number is subjected to a frequency substitution (104) and processed by an N-point inverse FFT (105). Thus, the signal becomes a real sequence signal of time domain, which is then digital-converted to be transmitted (107).

A descrambling process (11) of a reception part receiving a scrambled signal from
 25 the transmission part through a channel (108) is as follows.

The input analog signal is converted into a digital signal in the A/D converter (110) and subjected to the N-point FFT (111). Next, the FFT processed signal is processed with frequency inverse substitution by an inverse substitution algorithm (112) and the frequency inverse substituted signal is converted into a time domain signal through the N-
 30 point inverse FFT (113). The inverse FFT processed signal is converted ultimately into an analog signal in a digital to analog (D/A) converter and restored to an output signal to be output (115).

However, if the residual intelligibility is reduced using such FFT scrambling method,

the information to be transmitted contains some residual intelligibilities of the original signal due to the analog signal properties. To reduce such residual intelligibility sufficiently, it is necessary to scramble a signal by executing the FFT of at least 1024-point.

Moreover, in actual communications, it is necessary that an appropriate trade-off
5 between the FFT point number and the real-time process due to the increase and delay of calculation quantity according to the increase of FFT pointers.

Accordingly, the conventional FFT scrambling method has a problem in that the residual intelligibility of the original signal in the information to be protected is not sufficiently removed.

10

Technical Object of the Invention

Accordingly, an object of the present invention is to provide a method of fast Fourier transform scrambling and descrambling that scales the amplitude of signal in the fast Fourier transform pursuant to a substitution table produced in a transmission part in real
15 time and, then, scrambles the location of frequency component to modulate the location of frequency component as well as the amplitude of frequency component, thus reducing much more the residual intelligibility of the original signal and improving the safety of analog scrambler.

20

Composition and Effect of the Invention

A fast Fourier transform scrambling method in accordance with the present invention comprises the steps of: inputting an analog signal; converting the input analog signal into a digital signal; executing a fast Fourier transform to transform the digital signal to a frequency domain signal; executing an amplitude scaling for changing an amplitude
25 component of the frequency domain signal pursuant to a scaling table substituted using a substitution table produced from a substitution algorithm; substituting a location component of the frequency domain signal using the substitution table; executing an inverse fast Fourier transform to transform the frequency domain signal to a digital signal; and converting the digital signal to a scrambled analog signal to transmit.

30

A fast Fourier transform descrambling method in accordance with the present invention comprises the steps of: receiving a scrambled analog signal; converting the input scrambled analog signal into a digital signal; executing a fast Fourier transform to transform the digital signal to a frequency domain signal; restoring a location component of

the frequency domain signal using a substitution table produced from a substitution algorithm; executing an amplitude scaling to restore an amplitude component of the frequency domain signal pursuant to a scaling table substituted using the substitution table; executing an inverse fast Fourier transform to transform the frequency domain signal to a digital signal; and converting the digital signal into a not-scrambled analog signal.

A method of fast Fourier transform scrambling and descrambling in accordance with the present invention comprises the steps of: inputting an analog signal to a transmission part; converting the input analog signal into a digital signal; executing a fast Fourier transform to transform the digital signal to a frequency domain signal; executing an amplitude scaling for changing an amplitude component of the frequency domain signal pursuant to a scaling table substituted using a substitution table produced from a substitution algorithm; substituting a location component of the frequency domain signal using the substitution table; executing an inverse fast Fourier transform to transform the frequency domain signal to a digital signal; converting the digital signal to a scrambled analog signal; transmitting the scrambled analog signal from the transmission part to a reception part via a channel; receiving the scrambled analog signal in the reception part; converting the input scrambled analog signal into a digital signal; executing a fast Fourier transform to transform the digital signal to a frequency domain signal; restoring a location component of the frequency domain signal using a substitution table produced from a substitution algorithm; executing an amplitude scaling to restore an amplitude component of the frequency domain signal pursuant to a scaling table substituted using the substitution table; executing an inverse fast Fourier transform to transform the frequency domain signal to a digital signal; and converting the digital signal into a not-scrambled analog signal.

Moreover, the transmission and reception parts use the same substitution table and the same scaling table.

As described above, the present invention is directed to the method of fast Fourier transform scrambling and descrambling, in the process of FFT scrambling for an analog signal, which substitutes the scaling table previously provided using a substitution table (219) produced at every frames, before the transmission part substitutes the location of the frequency component, and scales the amplitude of frequency component by multiplying the amplitude of frequency component corresponding to the substituted scaling table, differently from the related art that handles only the location of frequency component

simply for the substitution, thus reducing the residual intelligibility of scrambled signal to be output ultimately. Subsequently, the reception part executes the process carried out by the transmission part conversely to restore the scaled frequency component.

Next, a detail description of the present invention will be given with reference to the attached drawings. The present invention is not restricted to the following embodiments, and many variations are possible within the spirit and scope of the present invention. The embodiments of the present invention are provided in order to more completely explain the present invention to anyone skilled in the art.

Fig. 2 is a conceptual diagram depicted for illustrating a method of fast Fourier transform scrambling and descrambling in accordance with the present invention.

Referring to the figure, in a scrambling process 20 of a transmission part, a real signal (201), an analog signal, of time domain input to a transmission end is sampled by an appropriate sampling frequency based on the sampling theorem, thus being converted into a digital signal (202).

Data generated as a result of an analog to digital (A/D) conversion is a discrete signal expressed in the unit of bit quantized when sampling. Such signal will be a sample data, i.e., a data unit to be processed digitally. The digital-converted data is converted into a frequency domain signal by executing an N-point FFT (203).

Next, an amplitude scaling operation (204) is executed to multiply a scaling table (220), substituted using a substitution table (219) produced from a substitution algorithm, by a frequency component to be amplitude-modulated, thus generating a signal, of which the amplitude of the frequency component is modulated.

Subsequently, the signal coefficient of frequency domain expressed by a complex number is subjected to a frequency substitution and, a location component of the frequency domain signal is substituted (205) according to the substitution table (219) and processed by an N-point inverse FFT (206). Thus, the signal becomes a real sequence signal of time domain, which is then analog-converted (207) to be transmitted (208).

A descrambling process (21) of a reception part receiving (210) a scrambled signal from the transmission part through a channel (209) is as follows.

The input analog signal is converted into a digital signal in the A/D converter (211) and subjected to the N-point FFT (212). Next, the FFT processed signal is processed with frequency inverse substitution by an inverse substitution algorithm (213) and amplitude of the changed frequency component (214) is restored using the same

substitution table (222), produced from the substitution algorithm, as the transmission part. The amplitude restored signal is converted into a signal of time domain by the process of N-point inverse FFT. The inverse FFT processed signal is converted ultimately into an analog signal in a digital to analog converter and restored to an output signal to be output (217).

Amplitude scaling operation of the transmission part and amplitude restoring operation of the reception part will now be described in detail with reference to Figs. 3 and 4.

Fig. 3 is a conceptual diagram depicted for illustrating the amplitude scaling operation of the transmission part in detail.

Referring to Fig. 3, first, the transmission part executes an N-point FFT (301) for an input signal to generate a signal of frequency domains of $f(0)$, $f(2)$, ..., $f(n)$ (302). In view of the fact that the transmission band of a general cable network is 300 to 3,400, only one frequency component (303) contained in the transmission band is to be substituted.

Next, a method of amplitude modulation is as follows.

A scaling table $[s(p(0)), s(p(1)), \dots, s(p(l-1))]$ (307) generated by substituting the locations of the respective values composed of an amplitude scaling table $[s(0), s(1), \dots, s(l-1)]$ previously produced (304) using a substitution table $[p(0), p(1), \dots, p(l-1)]$ (306) made from a substitution algorithm (305) is multiplied by the one frequency component (303) to generate a signal $[f(k)*s(p(0)), \dots, f(k+l-1)*s(p(l-1))]$ (308), of which the amplitude of frequency component is modulated from an original signal. Then, a general FFT scrambler process is carried out for the amplitude modulated signal (308).

Fig. 4 is a conceptual diagram depicted for illustrating the amplitude restoring operation of the reception part in detail.

Referring to Fig. 4, the reception part divides the location restored signal (402) via a frequency inverse substitution process (401) by frequency components (402) corresponding to a scaling table (406) generated by substituting the same scaling table $[s(p(0)), s(p(1)), \dots, s(p(l-1))]$ (403) as the transmission part using the same substitution table $[p(0), p(1), \dots, p(l-1)]$ (405) as the transmission part, produced from a substitution algorithm (404), thus obtaining a signal $[f(k)/s(p(0)), \dots, f(k+l-1)/s(p(l-1))]$ (407) corresponding to the original signal, of which the amplitude of the changed frequency components are restored.

Via the method of fast Fourier transform scrambling and descrambling method

described with reference to Figs. 2 to 4, it is possible to reduce the residual intelligibility of the original signal much more, thus protecting the information safely.

Meanwhile, it is possible to protect the scaling method concretely from a third party's illegal tap by executing the substitution using the substitution table generated by a safe substitution algorithm, not using the amplitude scaling table simply.

Moreover, it is possible to minimize the increase of calculation quantity by using the substitution table, at the same time, produced for substituting the frequency locations in the FFT scrambler, not generating the substitution table for substituting the amplitude scaling table using a separate substitution algorithm.

As described in detail above, the present invention has been disclosed herein with reference to preferred embodiments; however, it will be understood by those of ordinary skill in the art that various changes in form and details may be made without departing from the spirit and scope of the present invention as set forth in the following claims.

Effect of the Invention

According to the present invention, it is possible to reduce much more the residual intelligibility of the original signal, contained in the scrambling signal, without additional increase of calculation quantity in the transmission part by scaling the amplitude of the frequency using the substitution table, generated in order to substitute the frequency locations, thus protecting the information safely.

(57) SCOPE OF CLAIM

Claim 1.

A fast Fourier transform scrambling method comprising the steps of:

inputting an analog signal;

converting the input analog signal into a digital signal;

executing a fast Fourier transform to transform the digital signal to a frequency domain signal;

executing an amplitude scaling for changing an amplitude component of the frequency domain signal pursuant to a scaling table substituted using a substitution table produced from a substitution algorithm;

substituting a location component of the frequency domain signal using the substitution table;

executing an inverse fast Fourier transform to transform the frequency domain signal to a digital signal; and
converting the digital signal to a scrambled analog signal to transmit.

5 **Claim 2.**

The fast Fourier transform scrambling method as recited in claim 1,
wherein the substitution table and the scaling table are the same as those used when restoring the location component and the amplitude component of the frequency domain signal in the reception part.

10 **Claim 3**

A fast Fourier transform descrambling method comprising the steps of:

receiving a scrambled analog signal;

converting the input scrambled analog signal into a digital signal;

15 executing a fast Fourier transform to transform the digital signal to a frequency domain signal;

restoring a location component of the frequency domain signal using a substitution table produced from a substitution algorithm;

20 executing an amplitude scaling to restore an amplitude component of the frequency domain signal pursuant to a scaling table substituted using the substitution table;

executing an inverse fast Fourier transform to transform the frequency domain signal to a digital signal; and

converting the digital signal into a not-scrambled analog signal.

25 **Claim 4**

The fast Fourier transform descrambling method as recited in claim 3,

wherein the substitution table and the scaling table are the same as those used when restoring the location component and the amplitude component of the frequency domain signal in the reception part.

30 **Claim 5**

A method of fast Fourier transform scrambling and descrambling comprising the steps of:

inputting an analog signal to a transmission part;
converting the input analog signal into a digital signal;
executing a fast Fourier transform to transform the digital signal to a frequency
domain signal;

5 executing an amplitude scaling for changing an amplitude component of the
frequency domain signal pursuant to a scaling table substituted using a substitution table
produced from a substitution algorithm;

 substituting a location component of the frequency domain signal using the
substitution table;

10 executing an inverse fast Fourier transform to transform the frequency domain
signal to a digital signal;

 converting the digital signal to a scrambled analog signal;

 transmitting the scrambled analog signal from the transmission part to a reception
part via a channel;

15 receiving the scrambled analog signal in the reception part;

 converting the input scrambled analog signal into a digital signal;

 executing a fast Fourier transform to transform the digital signal to a frequency
domain signal;

 restoring a location component of the frequency domain signal using a substitution
20 table produced from a substitution algorithm;

 executing an amplitude scaling to restore an amplitude component of the frequency
domain signal pursuant to a scaling table substituted using the substitution table;

 executing an inverse fast Fourier transform to transform the frequency domain
signal to a digital signal; and

25 converting the digital signal into a not-scrambled analog signal.

Claim 6

The method of fast Fourier transform scrambling and descrambling as recited in
claim 5,

30 wherein the transmission and reception parts use the same scaling table and reuse
the substituting table, used for substituting the location, in the scaling table substitution.

(19)대한민국특허청(KR) (12) 공개특허공보(A)

(51) Int. Cl.⁷
H04K 1/04

(11) 공개번호 특2003-0083102
(43) 공개일자 2003년10월30일

(21) 출원번호 10-2002-0021506
(22) 출원일자 2002년04월19일

(71) 출원인 한국전자통신연구원
대전 유성구 가정동 161번지

(72) 발명자 손영호
대전광역시유성구송강동송강마을아파트203동205호
황인호
대전광역시서구만년동강변아파트109동902호

(74) 대리인 신영무

심사청구 : 있음

(54) 고속 퓨리에 변환 스크램블링 및 디스크램블링 방법

요약

본 발명은 고속 퓨리에 변환 스크램블링 및 디스크램블링 방법에 관한 것으로, 기존의 고속 퓨리에 스크램블링 방법에서 생성된 치환표에 따라 주파수 성분의 위치만을 스크램블링하는 것과 달리, 고속 퓨리에 변환이 이루어지는 신호의 진폭을 송신부에서 실시간으로 생성되는 치환표에 따라 먼저 스케일링 한 후 주파수 성분의 위치를 스크램블링 하여 주파수 성분의 위치뿐만 아니라 주파수 성분의 진폭까지도 추가로 변조함으로써, 원신호에 대한 잔여 이해도를 보다 더 감소시키고 아날로그 스크램블러 장비의 안전성을 강화시킬 수 있는 고속 퓨리에 변환 스크램블링 및 디스크램블링 방법이 개시된다.

대표도

도 2

색인어

고속 퓨리에 변환, 진폭 스케일링, 잔여 이해도, 치환표, 스케일링

명세서

도면의 간단한 설명

도 1은 종래의 고속 퓨리에 변환 스크램블링 및 디스크램블링 방법을 설명하기 위해 도시한 개념도이다.

도 2는 본 발명에 따른 고속 퓨리에 변환 스크램블링 및 디스크램블링 방법을 설명하기 위해 도시한 개념도이다.

도 3은 도 2의 송신부측 진폭 스케일링 동작을 보다 상세하게 설명하기 위해 도시한 세부 처리 개념도이다.

도 4는 도 2의 수신부측 진폭 복원 동작을 보다 상세하게 설명하기 위해 도시한 세부 처리 개념도이다.

<도면의 주요 부분에 대한 부호의 설명>

10, 20 : 스크램블링 과정 11, 21 : 디스크램블링 과정

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 고속 푸리에 변환 스크램블링 및 디스크램블링 방법에 관한 것으로, 특히 비화된 아날로그 신호에 존재하는 원신호에 대한 잔여 이해도(Residual intelligibility)를 감소시키기 위한 고속 푸리에 변환 스크램블링 및 디스크램블링 방법에 관한 것이다.

고속 푸리에 변환(Fast Fourier Transform; 이하 FFT라 함) 스크램블링(scrambling)이란 임의의 실수 신호를 전송할 때 이신호가 함축하고 있는 정보를 은닉하기 위해 사용하는 것을 말한다.

일반적으로 많이 사용하고 있는 아날로그 스크램블링 방법으로 FFT 스크램블링 방법이 있다.

FFT 스크램블링 방법은 공중전화망(PSTN) 등에서 단대단(End-to-end) 음성통신을 보호하기 위한 방식 중 아날로그 형태의 음성을 직접 비화 처리하는 아날로그 스크램블러 장비에 적용할 수 있는 기법으로, 전송 채널에서 비화음도청시 기존 아날로그 스크램블 방법보다 잔여 이해도를 더 감소시킬 수 있다.

FFT 스크램블러에서 음성을 비화시키는 방법은 입력된 음성신호를 FFT 변환 한 후 특정 암호 알고리즘에 의해 시간으로 생성되는 치환표에 따라 주파수 성분의 위치를 치환한 후 IFFT(Inverse FFT) 변환한 후 아날로그 신호 형태로 채널로 전송하게 된다.

이하, 첨부된 도면을 참조하여 종래 기술에 따른 고속 푸리에 변환 스크램블링 및 디스크램블링 방법을 설명하기로 한다.

도 1은 종래의 고속 푸리에 변환 스크램블링 및 디스크램블링 방법을 설명하기 위해 도시한 흐름도이다.

도 1을 참조하면, 송신부에서의 스크램블링 과정(10)은 먼저, 송신단으로 입력된 시간영역의 실수신호(아날로그 신호)는(101), 샘플링(Sampling) 이론에 근거하여 적절한 표본화 주파수로 표본화되어 디지털 신호로 변환된다(102). 이러한 아날로그/디지털(Analog/Digital; A/D) 변환의 결과로 생성되는 하나의 데이터는 샘플링시 양자화하는 비트 크기 단위로 표현되는 이산(Discrete) 신호이며, 이 신호가 하나의 샘플 데이터 즉, 디지털로 처리되는 데이터 단위가 된다. FFT 처리기에서는 디지털로 변환된 데이터를 크기가 N인 일정 블록으로 묶어 N-Point FFT 변환을 수행하여 주파수 영역의 신호로 변환한다(103). 복소수로 표현되는 주파수 영역의 신호 계수는 하나의 치환 대상이 되어 주파수 치환된 후(104), 다시 N-Point 역FFT 처리된다(105). 이에 의해 신호는 시간 영역의 실수 시퀀스 신호가 되며, 이는 다시 아날로그 변환되어(106) 송신(107)된다.

채널(108)을 통해 송신부로부터 스크램블링된 신호를 수신(109)받은 수신부의 디스크램블링 방법(11)은 다음과 같다.

아날로그 형태로 입력된신호는 A/D 변환기에서 디지털 신호로 변환되고(110), N-Point FFT 처리된다(111). 이후, FFT 처리된 신호는 역치환 알고리즘에 의하여 주파수 역치환되고(112), 주파수 역치환된 신호는 N-Point 역FFT 처리에 의해 시간 영역의 신호로 변환된다(113). 역FFT 처리된 신호는 D/A 변환기에서 최종적으로 아날로그 신호로 변환되어(114), 출력 신호로 복원된 후 출력되게 된다(115).

그러나, 이러한 FFT 스크램블링 방법을 이용하여 잔여 이해도를 감소시키더라도, 전송되는 정보에는 아날로그 신호의 특성으로 인하여 원신호의 잔여 이해도가 어느 정도는 존재하게 된다.

이러한 잔여 이해도를 충분히 줄이기 위해서는 신호를 적어도 1024-포인트 이상의 FFT 변환을 하여 스크램블 하여야 한다.

그러나, 실제 통신 시에는 FFT 포인트 증가에 따른 계산량 증가와 지연으로 인하여 실시간 처리라는 관점과 FFT 포인트 수간에 적당한 보완(Trade-off)이 이루어져야 한다.

따라서, 상기에서 서술한 종래의 FFT 스크램블링 방법은 실제 적용 시 보호되어야 할 정보에서 원신호에 대한 잔여 이해도를 충분히 제거하지 못하는 문제점이 있다.

발명이 이루고자 하는 기술적 과제

따라서, 본 발명은 상기의 문제점을 해결하기 위하여 고속 푸리에 변환이 이루어지는 신호의 진폭을 송신부에서 실시간으로 생성되는 치환표에 따라 먼저 스케일링 한 후 주파수 성분의 위치를 스크램블링 하여 주파수 성분의 위치 스크램블링을 하는 외에도 주파수 성분의 진폭까지도 추가로 변조함으로써, 원신호에 대한 잔여 이해도를 보다 더 감소시키고 아날로그 스크램블러 장비의 안전성을 강화시킬 수 있는 고속 푸리에 변환 스크램블링 및 디스크램블링 방법이 개시된다.

발명의 구성 및 작용

본 발명에 따른 고속 푸리에 변환 스크램블링 방법은 아날로그 신호가 입력되는 단계와, 아날로그 입력 신호를 디지털 신호로 변환하는 단계와, 고속 푸리에 변환을 수행하여 디지털 신호를 주파수 영역 신호로 변환하는 단계와, 치환 알고리즘으로부터 생성된 치환표를 이용하여 치환/생성된 스케일링 표에 따라 주파수 영역 신호의 진폭 성분이 변환되도록 진폭 스케일링을 수행하는 단계와, 동일한 치환표를 이용하여 주파수 영역 신호의 위치성분을 치환하는 단계와, 역 고속 푸리에 변환을 수행하여 주파수 영역 신호를 디지털 신호로 변환하는 단계, 및 디지털 신호를 아날로그 신호로 변환하는 단계를 포함하여 이루어지는 것을 특징으로 한다.

본 발명에 따른 고속 푸리에 변환 디스크램블링 방법은 비화된 아날로그 신호가 입력되는 단계와, 비화된 아날로그 입력 신호를 디지털 신호로 변환하는 단계와, 고속 푸리에 변환을 수행하여 디지털 신호를 주파수 영역 신호로 변환하는 단계와, 치환 알고리즘으로부터 생성된 치환표를 이용하여 주파수 영역 신호의 위치를 환원하는 단계와, 동일한 치환표를 이용하여 치환/생성된 스케일링 표에 따라 주파수 영역 신호의 진폭 성분이 복원되도록 진폭 스케일링을 수행하는 단계와, 역 고속 푸리에 변환을 수행하여 주파수 영역 신호를 디지털 신호로 변환하는 단계, 및 디지털 신호를 비화되지 않은 아날로그 신호로 변환하는 단계를 포함하여 이루어지는 것을 특징으로 한다.

본 발명에 따른 고속 푸리에 변환 스크램블링 방법 및 디스크램블링 방법은 송신부로 아날로그 신호가 입력되는 단계와, 아날로그 입력 신호를 디지털 신호로 변환하는 단계와, 고속 푸리에 변환을 수행하여 디지털 신호를 주파수 영역 신호로 변환하는 단계와, 치환 알고리즘으로부터 생성된 치환표를 이용하여 치환/생성된 스케일링 표에 따라 주파수 영역 신호의 진폭 성분이 변환되도록 진폭 스케일링을 수행하는 단계와, 치환표를 이용하여 주파수 영역 신호의 위치성분을 치환하는 단계와, 역 고속 푸리에 변환을 수행하여 주파수 영역 신호를 디지털 신호로 변환하는 단계와, 디지털 신호를 비화된 아날로그 신호로 변환하는 단계, 채널을 통해 비화된 아날로그 신호를 송신부로부터 수신부로 전송하는 단계와, 수신부로 비화된 아날로그 신호가 입력되는 단계와, 비화된 아날로그 입력 신호를 디지털 신호로 변환하는 단계와, 고속 푸리에 변환을 수행하여 디지털 신호를 주파수 영역 신호로 변환하는 단계와, 치환 알고리즘으로부터 생성된 치환표를 이용하여 주파수 영역 신호의 위치를 환원하는 단계와, 동일한 치환표를 이용하여 치환/생성된 스케일링 표에 따라 주파수 영역 신호의 진폭 성분이 복원되도록 진폭 스케일링을 수행하는 단계와, 역 고속 푸리에 변환을 수행하여 주파수 영역 신호를 디지털 신호로 변환하는 단계, 및 디지털 신호를 비화되지 않은 아날로그 신호로 변환하는 단계를 포함하는 것을 특징으로 한다.

상기에서, 송신부 및 수신부는 동일한 치환표 및 스케일링 표를 사용하는 것을 특징으로 한다.

상기와 같이, 본 발명은 아날로그 신호에 대한 FFT 스크램블링 처리 과정에서, 종래 기술에서와 같이 단순히 주파수 성분의 위치만을 치환대상으로 취급하지 않고, 송신부측에서 주파수 성분의 위치를 치환하기 전에 매 프레임마다 생성되는 치환표(219)를 이용하여 사전에 만들어진 스케일링 표를 먼저 치환한 후 대응되는 주파수 성분의 진폭에 곱하여 먼저 주파수 성분의 진폭을 스케일링하는 과정을 첨가함으로써 최종적으로 출력되는 비화 신호의 잔여 이해도를 감소시키고자 하는 것이다. 그리고, 수신부측에서는 송신부측에서 실시한 과정을 반대로 수행하여 스케일링된 주파수 성분을 복원하게 된다.

이하, 첨부된 도면을 참조하여 본 발명의 실시예를 보다 더 상세히 설명하기로 한다.

도 2는 본 발명에 따른 고속 푸리에 변환 스크램블링 및 디스크램블링 방법을 설명하기 위해 도시한 흐름도이다.

도 2를 참조하면, 먼저 송신부에서의 스크램블링 과정(20)은 송신단으로 입력된 시간영역의 실수신호(아날로그 신호)는(201), 샘플링 이론에 근거하여 적절한 표본화 주파수로 표본화되어 디지털 신호로 변환된다(202). 이러한 아날로그/디지털(Analog/Digital; A/D) 변환의 결과로 생성되는 하나의 데이터는 샘플링시 양자화하는 비트 크기 단위로 표현되는 이산(Discrete) 신호이며, 이 신호가 하나의 샘플 데이터 즉, 디지털로 처리되는 데이터 단위가 된다. FFT 처리기에서는 디지털로 변환된 데이터를 크기가 N인 일정 블록으로 묶어 N-Point FFT 변환을 수행하여 주파수 영역의 신호로 변환한다(203).

이후, 치환 알고리즘(218)으로부터 생성된 치환표(219)를 이용하여 치환/생성된 스케일링 표(220)를 진폭 변조 대상인 주파수 성분과 곱함으로써 원 신호에서 주파수 성분의 진폭이 변조된 신호를 생성하는 진폭 스케일링 동작을 실시(204)한다.

이어서, 복소수로 표현되는 주파수 영역의 신호 계수는 하나의 치환 대상이 되어, 치환표(219)에 따라 주파수 영역 신호의 위치 성분이 치환된 후(205), 다시 N-Point 역FFT 처리된다(206). 이에 의해 신호는 시간 영역의 실수 시퀀스 신호가 되며, 이는 다시 아날로그 변환되어(207) 송신(208)된다.

채널(209)을 통해 송신부으로부터 스크램블링된 신호를 수신(210)받은 수신부의 디스크램블링 방법(21)은 다음과 같다.

아날로그 형태로 입력된 신호는 A/D 변환기에서 디지털 신호로 변환되고(211), N-Point FFT 처리된다(212). 이후, FFT 처리된 신호는 역치환 알고리즘에 의하여 주파수 역변환되고(213), 위치가 복원된 신호를 대상으로 송신부측과 동일한 스케일링 표(220)를 치환 알고리즘(221)으로 생성된 송신측과의 동일한 치환표(222)를 이용하여 변형된 주파수 성분의 진폭을 복원(214)한다. 진폭이 복원된 신호는 N-Point 역FFT 처리에 의해 시간 영역의 신호로 변환된다(215). 역FFT 처리된 신호는 D/A 변환기에서 최종적으로 아날로그 신호로 변환되어(216), 출력 신호로 복원된 후 출력되게 된다(217).

도 2에서 송신부측의 진폭 스케일링 동작과 수신부측의 진폭 복원 동작을 나누어 상세하게 설명하면 다음과 같다.

도 3은 도 2의 송신부측 진폭 스케일링 동작을 보다 상세하게 설명하기 위해 도시한 세부 처리 흐름도이다.

도 3을 참조하면, 먼저 송신부측에서는 매 프레임마다 입력되는 신호를 N-point FFT(301)를 수행함으로써 $f(0)$, $f(1)$, ..., $f(n)$ 의 주파수 영역에서의 신호(302)를 생성한다. 그리고, 일반적인 유선망의 전송 대역이 300 내지 3400 인 점을 고려하여, 전송 대역에 포함되는 주파수 성분 1개(303)만을 치환 대상으로 한다.

이후, 진폭 변조의 방법을 설명하면, 사전에 생성된 진폭 스케일링 표 $\{s(0), s(1), \dots, s(l-1)\}$ 를 구성(304)하는 각 값들의 위치를 치환 알고리즘(305)으로부터 생성된 치환표 $\{p(0), p(1), \dots, p(l-1)\}$ (306)를 이용하여 치환하여 생성된 스케일링 표 $\{s(p(0)), s(p(1)), \dots, s(p(l-1))\}$ (307)를 진폭 변조 대상인 주파수 성분 1개(303)와 곱함으로써 원 신호에서 주파수 성분의 진폭을 변조한 신호 $\{f(k)*s(p(0)), \dots, f(k+l-1)*s(p(l-1))\}$ 가 생성(308)된다. 그리고, 진폭이 변조된 신호(308)를 대상으로 일반적인 FFT 스크램블러 과정을 적용하게 된다.

도 4는 도 2의 수신부측 진폭 복원 동작을 보다 상세하게 설명하기 위해 도시한 세부 처리 흐름도이다.

도 4를 참조하면, 수신부측에서는 먼저 주파수 성분 역 치환 과정(401)을 거쳐서 위치가 복원된 신호(402)를 대상으로 송신측과 동일한 스케일링 표 $\{s(0), s(1), \dots, s(l-1)\}$ (403)를 치환 알고리즘(404)으로 생성된 송신측과의 동일한 치환표 $\{p(0), p(1), \dots, p(l-1)\}$ (405)를 이용하여 먼저 치환하여 생성된 스케일링 표(406)를 대응되는 주파수 성분(402)에 나누어줌으로써 변형된 주파수 성분의 진폭을 복원한 원 신호에 해당하는 $\{f(k)/s(p(0)), \dots, f(k+l-1)/s(p(l-1))\}$ (407)를 얻도록 구성되게 된다.

도 2 내지 도 4를 참조하여 설명한 고속 푸리에 변환 스크램블링 및 디스크램블링 방법을 통해 원신호에 대한 잔여 이해도를 보다 더 감소시켜 정보를 안전하게 보호할 수 있다.

한편, 진폭 스케일링 표를 단순히 사용하지 않고 안전한 치환 알고리즘으로 생성된 치환표를 사용하여 치환함으로써 제 3자의 불법 도청으로부터 구체적인 스케일링 방법이 안전하게 보호된다.

또한, 진폭 스케일링 표를 치환하기 위한 치환표를 별도의 치환 알고리즘을 이용하여 생성하지 않고 FFT 스크램블러에서 주파수 위치를 치환하기 위하여 생성하는 치환표를 함께 사용함으로써 계산량 증가를 최소화할 수 있다.

발명의 효과

상술한 바와 같이, 본 발명은 주파수 위치를 치환하는데 사용하기 위하여 생성되는 치환표로 주파수의 진폭까지 스케일링함으로써, 송수신부에서 별도의 계산량 증가없이 비화 신호에 포함된 원신호에 대한 잔여 이해도를 보다 더 감소시켜 정보를 안전하게 보호할 수 있다.

(57) 청구의 범위

청구항 1.

아날로그 신호가 입력되는 단계;

상기 아날로그 입력 신호를 디지털 신호로 변환하는 단계;

고속 푸리에 변환을 수행하여 상기 디지털 신호를 주파수 영역 신호로 변환하는 단계;

치환 알고리즘으로부터 생성된 치환표를 이용하여 치환/생성된 스케일링 표에 따라 상기 주파수 영역 신호의 진폭 성분이 변환되도록 진폭 스케일링을 수행하는 단계;

상기 치환표를 이용하여 상기 주파수 영역 신호의 위치성분을 치환하는 단계;

역 고속 푸리에 변환을 수행하여 상기 주파수 영역 신호를 디지털 신호로 변환하는 단계; 및

상기 디지털 신호를 비화된 아날로그 신호로 변환하여 송신하는 단계를 포함하여 이루어지는 것을 특징으로 하는 고속 푸리에 변환 스크램블링 방법.

청구항 2.

제 1 항에 있어서, 상기 치환표 및 상기 스케일링 표는 수신부에서 상기 주파수 영역 신호의 상기 위치 성분 및 상기 진폭 성분을 복원할 때 사용되는 것과 동일한 것을 특징으로 하는 고속 푸리에 변환 스크램블링 방법.

청구항 3.

비화된 아날로그 신호가 수신되는 단계;

상기 비화된 아날로그 입력 신호를 디지털 신호로 변환하는 단계;

고속 푸리에 변환을 수행하여 상기 디지털 신호를 주파수 영역 신호로 변환하는 단계;

치환 알고리즘으로부터 생성된 치환표를 이용하여 상기 주파수 영역 신호의 위치성분을 환원하는 단계;

상기 치환표를 이용하여 치환/생성된 스케일링 표에 따라 상기 주파수 영역 신호의 진폭 성분이 복원되도록 진폭 스케일링을 수행하는 단계;

역 고속 푸리에 변환을 수행하여 상기 주파수 영역 신호를 디지털 신호로 변환하는 단계; 및

상기 디지털 신호를 비화되지 않은 아날로그 신호로 변환하는 단계를 포함하여 이루어지는 것을 특징으로 하는 고속 푸리에 변환 디스크램블링 방법.

청구항 4.

제 3 항에 있어서, 상기 치환표 및 상기 스케일링 표는 송신부에서 상기 주파수 영역 신호의 상기 위치 성분 및 상기 진폭 성분을 변조할 때 사용된 것과 동일한 것을 특징으로 하는 고속 푸리에 변환 디스크램블링 방법.

청구항 5.

송신부로 아날로그 신호가 입력되는 단계;

상기 아날로그 입력 신호를 디지털 신호로 변환하는 단계;

고속 푸리에 변환을 수행하여 상기 디지털 신호를 주파수 영역 신호로 변환 하는 단계;

치환 알고리즘으로부터 생성된 치환표를 이용하여 치환/생성된 스케일링 표에 따라 상기 주파수 영역 신호의 진폭 성분이 변환되도록 진폭 스케일링을 수행하는 단계;

상기 치환표를 이용하여 상기 주파수 영역 신호의 위치성분을 치환하는 단계;

역 고속 푸리에 변환을 수행하여 상기 주파수 영역 신호를 디지털 신호로 변환하는 단계;

상기 디지털 신호를 비화된 아날로그 신호로 변환하는 단계

채널을 통해 상기 비화된 아날로그 신호를 상기 송신부로부터 수신부로 전송하는 단계;

상기 수신부로 비화된 아날로그 신호가 입력되는 단계;

상기 비화된 아날로그 입력 신호를 디지털 신호로 변환하는 단계;

고속 푸리에 변환을 수행하여 상기 디지털 신호를 주파수 영역 신호로 변환하는 단계;

상기 치환 알고리즘으로부터 생성된 상기 치환표를 이용하여 상기 주파수 영역 신호의 위치성분을 환원하는 단계;

상기 치환표를 이용하여 치환/생성된 상기 스케일링 표에 따라 상기 주파수 영역 신호의 진폭 성분이 복원되도록 진폭 스케일링을 수행하는 단계;

역 고속 푸리에 변환을 수행하여 상기 주파수 영역 신호를 디지털 신호로 변환하는 단계; 및

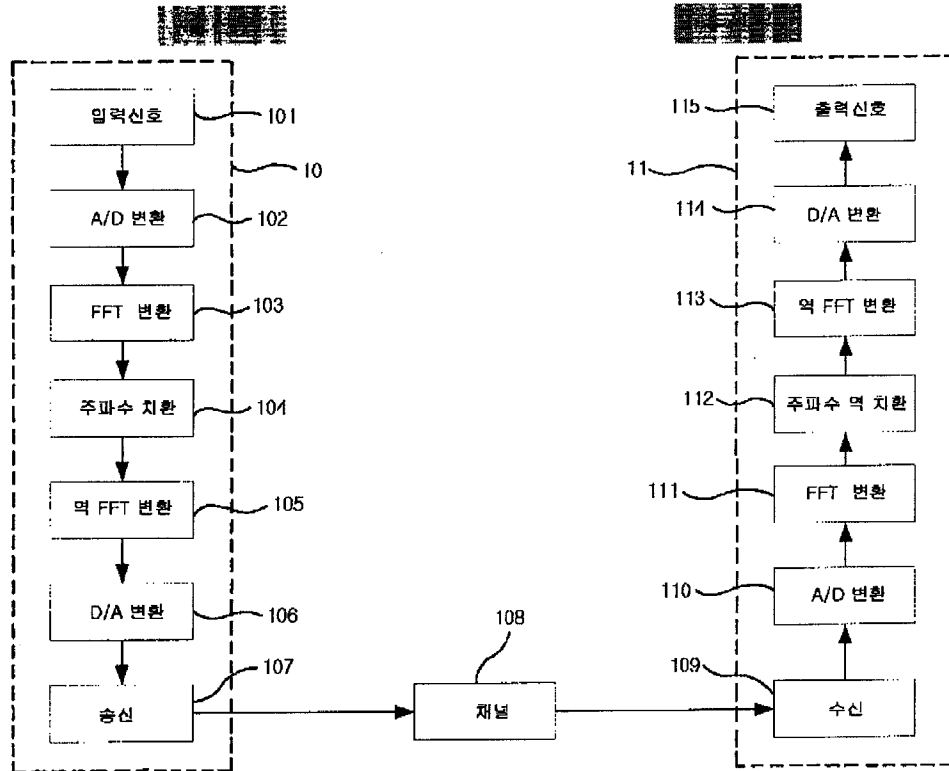
상기 디지털 신호를 비화되지 않은 아날로그 신호로 변환하는 단계를 포함하는 것을 특징으로 하는 고속 푸리에 변환 스크램블링 및 디스크램블링 방법.

청구항 6.

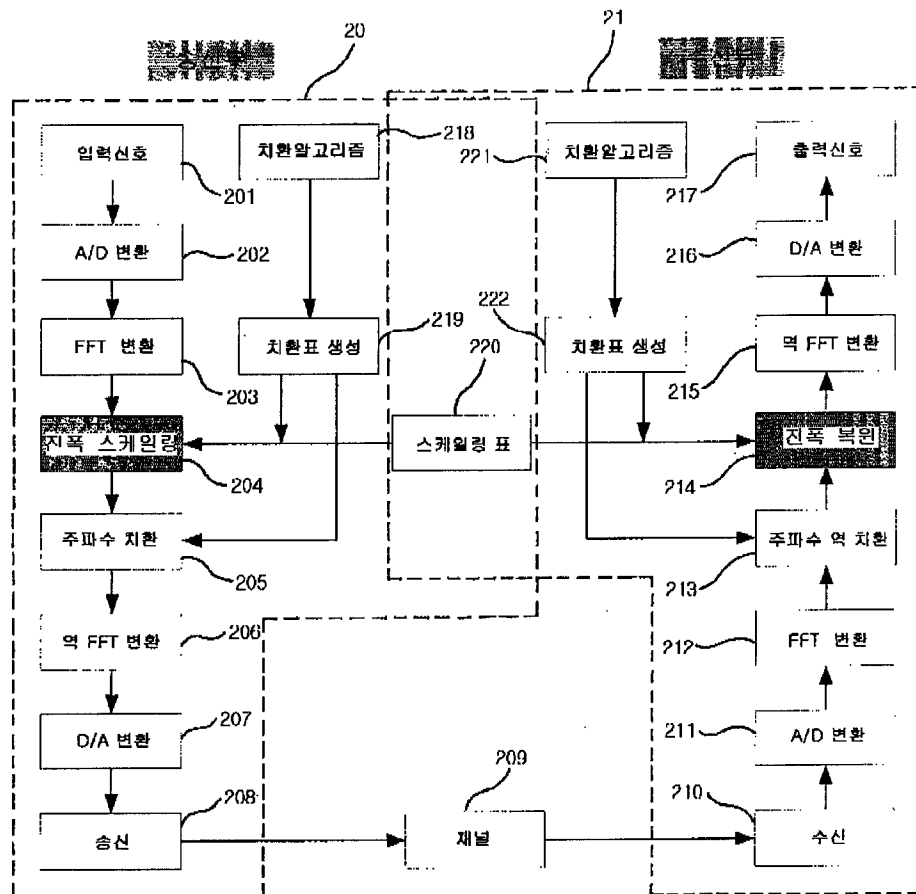
제 5 항에 있어서, 상기 송신부 및 상기 수신부는 동일한 스케일링 표를 사용하고 위치 치환에 사용된 치환표를 상기 스케일링 표 치환에 재사용한 것을 특징으로 하는 고속 푸리에 변환 스크램블링 및 디스크램블링 방법.

도면

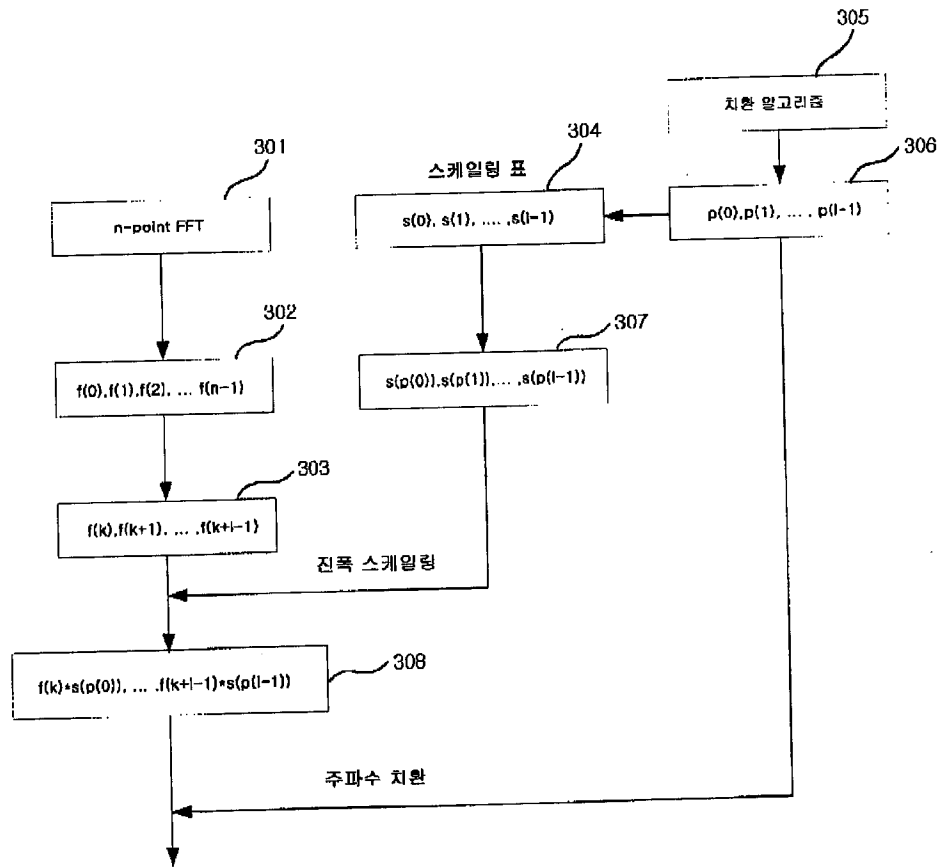
도면1



도면2



도면3



도면4

